Exam : **C2090-623**

Title : IBM Cognos Analytics Administrator V1

Version : Demo

1.An administrator needs to setup security for a newly installed environment.
Which of the following is a valid step?
A. Remove the default authentication provider.
B. Enable anonymous access for selected users, groups, or roles.
C. Delete the Everyone group to limit access to the environment for selected users, groups, and roles.
D. Add trusted users, groups, or roles to the System Administrators role, and then remove the Everyone group from the role.
Answer: D
Explanation:
You may not want all users that exist in an authentication source to have access to IBM Cognos software. To secure IBM Cognos software, configure the product so that only users who belong to a specific group or role in your authentication source, or in the Cognos namespace, are allowed access.
We recommend using the Cognos namespace because it contains preconfigured groups and roles that help you to secure IBM Cognos software quickly. One of the preconfigured groups is Everyone.
By default, the group Everyone belongs to several built-in groups and roles in the Cognos namespace.
If you decide to use the Cognos namespace, you must remove the Everyone group from all built-in groups and roles and replace it with groups, roles, or users authorized to access IBM Cognos software.
References: IBM Cognos Administration Version 10.1.0, Administration and Security Guide, page 64

2.In a multi-server environment, an administrator wants to ensure that items in the Content Manager Cache service are re-validated every thirty seconds.
Which option would accomplish this?
A. Set the memory limit of the Content Manager Cache service to 30000.
B. Set the DISP.contentManagerCacheService.accountInactivityTimer property to 30000.
C. Set the DISP.contentManagerCacheService.cacheValidatorTimetoLive property to 30000.
D. Set the DISP.contentManagerCacheService.cacheValidatorTimetoLinger property to 30000.
Answer: C
Explanation:
ValidatorTimetoLive determines how long data objects remain in the cache. After the Validator timer expires objects are considered Invalid and have to be fetched from Cm again. Value is in ms, and default is 900000.
References: https://www.slideshare.net/barnaby1502/cognos-technical-super-session-2012, page 11

3.An administrator is configuring settings for the Cognos Analytics Mobile app.
Which settings can be managed?
A. To store the user credentials in the IBM Cognos Mobile app.
B. The maximum number of minutes to store cached credentials.
C. Allow the user to create an image (screenshot) of the Active Report.
D. The maximum number of Active Reports to store locally on the mobile device.
Answer: B
Explanation:
Policy settings
These settings define how to deliver Cognos Analytics content to mobile applications.
References:

https://www.ibm.eom/support/knowledgecenter/en/SSEP7J_11.0.0/com.ibm.swg.ba.cognos.ug_cra.doc/c_mob_global_config_settings.html

4.An administrator is evaluating system status using the Scorecard pane on the Status > System page in the IBM Cognos Administration console.
Which statement is true?
A. If a service is disabled in IBM Cognos Configuration, it is listed in the Scorecard pane.
B. The status that is displayed for each entry reflects the lowest status for all child entries.
C. A status of Available is displayed when at least 80% of the child entries have a status of Available.
D. A status of Unavailable is displayed when at least 80% of the child entries have a status of Unavailable.
Answer: B
Explanation:
The metric score for each entry is based on the performance of individual child entries. The status that is displayed for each entry is the lowest status of the child entries. For example, if all the metrics for a dispatcher are good, but one service on that dispatcher has a poor metric, the metric score shown for the dispatcher is poor.
Status is one of the following:
References:
https://www.ibm.eom/support/knowledgecenter/SSEP7J_11.0.0/com.ibm.swg.ba.cognos.ug_cra.doc/c_panes_system_status_page.html

5.An administrator is implementing security by managing and working with the Cognos namespace.
Which statement is true?
A. To gain access to IBM Cognos Analytics, users can log on to the Cognos namespace.
B. Create domain users in the Cognos namespace to avoid cluttering the existing authentication provider.
C. User-defined groups and roles must be created in a 3rd-party authentication provider and cannot be created in the Cognos namespace.
D. Although the use of the predefined and built-in groups and roles within the Cognos namespace is optional, the Cognos namespace cannot be deleted.
Answer: D
Explanation:
The Cognos namespace includes predefined objects to help you quickly set up initial security.
You use the predefined objects and other features of the Cognos namespace for ongoing security management.
You can create groups and roles in the Cognos namespace.
initial access permissions are applied to all predefined objects. You can modify the permissions from the object properties.
References:
https://www.ibm.com/support/knowledgecenter/en/SSEP7J_11.0.0/com.ibm.swg.ba.cognos .ag_manage.doc/c_ca_cognos_namespace.html